

In the Claims:

Please cancel claims 4-7. Please amend claim 3. Please add new claims 23-26. The claims are as follows:

1. (Original) A method of operating an intrusion detection system, the method comprising the steps of:

taking a base action in response to detecting an intrusion;

updating an action counter in response to taking the base action;

comparing the value of the action counter to an action threshold;

updating an action variable when the value of the action counter meets the action

threshold;

checking a validity condition for satisfaction dependent upon the action variable; and

invoking a provision associated with the validity condition when the validity condition is satisfied.

2. (Original) The method of claim 1, wherein the provision changes an element of a base intrusion set.

3. (Currently amended) ~~The method of claim 2;~~ A method of operating an intrusion detection system, the method comprising the steps of:

taking a base action in response to detecting an intrusion;

updating an action counter in response to taking the base action;

comparing the value of the action counter to an action threshold;
updating an action variable when the value of the action counter meets the action
threshold;
checking a validity condition for satisfaction dependent upon the action variable; and
invoking a provision associated with the validity condition when the validity condition is
satisfied, wherein the provision changes an element of a base intrusion set, and wherein the
element of the base intrusion set is selected from the group consisting of a signature event, a
signature event counter, a signature threshold, a base action, and a weight.

4-7. (Canceled)

8. (Original) The method of claim 1, wherein the provision changes an element of an action set.
9. (Original) The method of claim 8, wherein the element of the action set is an action counter.
10. (Original) The method of claim 8, wherein the element of the action set is an action threshold.
11. (Original) The method of claim 8, wherein the element of the action set is an action variable.
12. (Original) A method of operating an intrusion detection system, the method comprising the steps of:

09/901,443

detecting a signature event;
updating a signature event counter responsive to detecting the signature event;
comparing the value of the signature event counter to a signature threshold;
updating an action counter when the value of the signature event counter meets the signature threshold;
comparing the value of the action counter to an action threshold;
updating an action variable when the value of the action counter meets the action threshold;
checking a validity condition for satisfaction dependent upon the action variable; and
invoking a provision associated with the validity condition when the validity condition is satisfied.

13. (Original) The method of claim 12, wherein the provision changes an element of a base intrusion set.

14. (Original) The method of claim 13, wherein the element of the base intrusion set is a signature event.

15. (Original) The method of claim 13, wherein the element of the base intrusion set is a signature event counter.

16. (Original) The method of claim 13, wherein the element of the base intrusion set is a

signature threshold.

17. (Original) The method of claim 13, wherein the element of the base intrusion set is a base action.

18. (Original) The method of claim 13, wherein the element of the base intrusion set is a weight.

19. (Original) The method of claim 12, wherein the provision changes an element of an action set.

20. (Original) The method of claim 19, wherein the element of the action set is an action counter.

21. (Original) The method of claim 19, wherein the element of the action set is an action threshold.

22. (Original) The method of claim 19, wherein the element of the action set is an action variable.

23. (New) The method of claim 1, wherein the action variable is selected from the group consisting of a binary variable, an integer variable, a floating point variable, a fuzzy logical variable, and a M-ary variable.

09/901,443

5

24. (New) The method of claim 1, wherein the validity condition includes a mathematical expression or a logical expression.

25. (New) The method of claim 1, wherein said checking step comprises checking the validity condition for satisfaction dependent upon the action variable and upon at least one other action variable.

26. (New) The method of claim 1, further comprising a plurality of rules, wherein a rule of the plurality of rules comprises the validity condition.